# Department of Homeland Security
## Information Analysis and Infrastructure Protection Directorate
# CyberNotes

*Issue #2003-08* *April 21, 2003*

**CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between April 1 and April 18, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| 12Planet[1] | Windows NT 4.0/2000, XP, Unix | Chat Server 2.5 | Two vulnerabilities exist: a vulnerability exists because the administration login page passes authentication information in cleartext, which could let a remote malicious obtain administrative access; and a path disclosure vulnerability exists when certain malformed URL requests are submitted, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Chat Server Cleartext Authentication & Path Disclosure | Medium/ **High** **(High if adminis-trative access can be obtained)** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[1] Securiteam, April 18, 20003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| access referer. source-forge.net[2] | Unix | Apache mod_ access_ referer 1.0.2 | A remote Denial of Service vulnerability exists in the find_allowdeny() function when parsing invalid HTTP referer header fields. | No workaround or patch available at time of publishing. | Apache Mod_Access_ Referer Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| ActivCard Corpora-tion[3] | Windows XP | ActivCard Gold 1.21, 2.2 | A vulnerability exists because static passwords are cached in memory, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | ActivCard Gold Cached Static Password | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| AMaViS[4] | Unix | AMaViS-ng 0.1.6.1-0.1.6 .3 | A vulnerability exists because AMaViS-ng does not properly interact with Postfix, which could let a malicious user circumvent relay restrictions. | No workaround or patch available at time of publishing. | AMaViS Relaying Restrictions Circumvention | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Apache Software Founda-tion[5] | OS2 | Apache 2.0.35-2.0.45 | A Denial of Service vulnerability exists because device names can fault the OS2 worker process. | Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.45/os2_filestat_security_fix.patch | Apache Web Server OS2 Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Apple[6] | MacOS X 10.x | MacOS X 10.0-10.2.4, MacOS X Server 10.0, 10.2-10.2.4 | A vulnerability exists in Directory Service daemon due to the way the libc system() function is used to execute commands, which could let a malicious user obtain elevated privileges. | Upgrade available at: http://docs.info.apple.com/article.html?artnum=120211 | MacOS X Directory Service Privilege Escalation<br><br>CVE Name: CAN-2003-0171 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Apple[7] | MacOS X 10.x | MacOS X 10.0-10.2.4, MacOS X Server 10.0, 10.2-10.2.4 | A remote Denial of Service vulnerability exists in the Directory Service daemon when a malicious user repeatedly connects to specific network ports. | Upgrade available at: http://docs.info.apple.com/article.html?artnum=120211 | MacOS X Directory Service Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Apple[8] | MacOS X 10.x | MacOS X 10.0-10.2.4, MacOS X Server 10.0, 10.2-10.2.4 | An information disclosure vulnerability exists in the way privileges are granted to 'guest' users when shared folders are accessed, which could let a malicious user obtain sensitive information. | Upgrade available at: http://docs.info.apple.com/article.html?artnum=120211 | MacOS X Information Disclosure<br><br>CVE Name: CAN-2003-0198 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[2] Safemode.org Security Advisory, April 16, 2003.
[3] Bugtraq, April 14, 2003.
[4] SecurityFocus, April 10, 2003.
[5] Bugtraq, April 11, 2003.
[6] @stake, Inc. Security Advisory, a041003-1, April 10, 2003.
[7] @stake, Inc. Security Advisory, a041003-1, April 10, 2003.
[8] Apple Security Update, 61798, April 10, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Aprelium Technol-ogies[9] | Windows, Unix | Abyss Web Server 1.1.2 | A remote Denial of Service vulnerability exists because invalid HTTP requests are not handled properly | Upgrade available at: http://www.aprelium.com/abyssws/download.php | Abyss Web Server Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Proofs of Concept exploit have been published. |
| Ashley Brown[10] | Windows NT | iWeb Server | A Directory Traversal vulnerability exists due to insufficient validation of client requested paths, which could let a remote malicious user obtain sensitive information. | Upgrade available at: http://www.ashleybrown.co.uk/downloads/iws2.exe | iWeb Server Directory Traversal | Medium | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| AStArt Technol-ogies[11] | Unix | LPRng 3.8.10 .1 | A vulnerability exists in the 'psbanner' filter because temporary files for debugging purposes are created insecurely, which could let a malicious user obtain elevated privileges. | **Debian:** http://security.debian.org/pool/updates/main/l/lprng/ | LPRng 'PSBanner' Insecure Temporary File Creation<br><br>CVE Name: CAN-2003-0136 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Auto-mated Shops[12] | Windows, Unix | WebC 2.0 11, 5.0 05, 5.0 | Several vulnerabilities exist: a buffer overflow vulnerability exists because certain configuration files are not processed safely, which could let a remote malicious user obtain unauthorized access and execute arbitrary code; a symbolic link vulnerability exists, which could let a malicious user execute arbitrary files; and a buffer overflow vulnerability exists in the WebC.cgi application when the user ID is changed during runtime (if debugging is enabled), which could let a remote malicious execute arbitrary code. | Upgrade available at: ftp://ftp.automatedshops.com/pub/webc/5.020/ | WebC Multiple Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. |
| Bajie[13] | Windows | Java HTTP Server 0.95 zxe, zxc | A Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML and script code from error output, which could let a remote malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. | Bajie Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[9] SecurityTracker Alert ID, 1006489, April 5, 2003.
[10] Securiteam, April 18, 2003.
[11] Debian Security Advisory, DSA 285-1, April 14, 2003.
[12] Bugtraq, April 3, 2003.
[13] SecurityTracker Alert ID. 1006428, April 1, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| BitchX[14] | Multiple | IRC Client 1.0 c19 | The server that hosts BitchX (www.bitchx.org) was recently compromised and the intruder made modifications to the source code to include Trojan horse code. Once the Trojan is executed, it attempts to connect to host 207.178.61.5 on port 6667. The Trojan horse modifications can be found in the configure script. | No workaround or patch available at time of publishing. | BitchX Trojan Horse | **High** | Bug discussed in newsgroups and websites. |
| Bitstrike Software[15] | Windows NT 4.0/2000 | Sign Here! Guestbook | A vulnerability exists in the 'Default.asp' script due to a failure to filter user-supplied input via the E-mail field, which could let a malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. | Sign Here! Guestbook 'Default.asp' | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Borland/ Inprise[16] | Unix | Interbase 6.0, 6.4, 6.5; Firebird Firebird 1.0.2 | A vulnerability exists due to insufficient checks when external databases are created or manipulated, which could let a malicious user execute arbitrary code with root privileges. | This vulnerability does not affect Interbase 7.0. Affected users are advised to upgrade. | Interbase External Table File Verification | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Borland/ Inprise[17] | Windows NT 4.0/2000, Unix | Interbase 6.0, 6.4, 6.5; Firebird Firebird 1.0.2 | A buffer overflow vulnerability exists in the gds_lock_mgr program, which could let a malicious user execute arbitrary code as root. | No workaround or patch available at time of publishing. | Interbase GDS_Lock_ MGR Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Boutell. com[18] | Unix | rinetd 0.61, 0.52 | A vulnerability exists in the 'rinetd' TCP redirection tool, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. | **inetd:** http://www.boutell.com/rinetd/http/rinetd.tar.gz **Debian:** http://security.debian.org/pool/updates/main/r/rinetd/ | Rinetd TCP Redirection CVE Name: CAN-2003-0212 | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |

[14] SecurityFocus, April 13, 2003.
[15] Black Tigerz Research Group Advisory, April 4, 2003.
[16] Secunia Security Advisory, April 9, 2003.
[17] Secure Network Operations, Inc. Advisory, SRT2003-04-03-1300, April 3, 2003.
[18] Debian Security Advisory, DSA 289-1, April 17, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| BRS[19] | Windows 98 | Web Weaver 1.01-1.03 | Several vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a request for a URL that contains excessive data; a vulnerability exists in the 'testcgi.exe' sample application, which could let a malicious user obtain sensitive information; and a vulnerability exists in the encryption scheme used to store encoded passwords, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | WebWeaver Multiple Vulnerabilities | Low/ Medium (Medium if sensitive informa-tion can be obtained) | Bug discussed in newsgroups and websites. Denial of Service vulnerability can be exploited via a web browser or text-based network client such as Telnet or netcat. |
| Buffalo Technol-ogy[20] | Multiple | Wireless Broadband Router WBRG54 1.13, 1.11 | A Denial of Service vulnerability exists when a malicious user submits numerous ICMP packets to the device. | No workaround or patch available at time of publishing. | Wireless Broadband Router WBRG54 Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Cerberus[21] | Multiple | FTP Server 2.1 | An information disclosure vulnerability exists due the way the authentication procedure is handled, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Cerberus FTP Server Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Chindi[22] | Windows | Chindi Build 1182 | A remote Denial of Service vulnerability exists when a malicious user submits an excessively long request. | No workaround or patch available at time of publishing. | Chindi Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Christian Void[23] | Unix | passlogd 0.1a-0.1d | Multiple buffer overflow vulnerabilities exist in the sl_parse() function, which could let a remote malicious user execute arbitrary code. | Upgrade available at: http://www.morphine.com/src/passlogd-0.1e.tar.gz | Passlog Daemon SL_Parse Remote Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |

[19] Secunia Security Advisory, April 4, 2003.
[20] Bugtraq, April 3, 2003.
[21] SecurityFocus, April 16, 2003.
[22] SecurityFocus, April 14, 2003.
[23] INetCop Security Advisory, 2003-0x82-015, April 3, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Citrix[24] | Windows, MacOS X, Unix | ICA Client for Linux 6.30.1053, 6.30.1054, 6.30.1056, ICA Client for OS X 6.30.314, ICA Client for Solaris/ Sparc 6.30.1061, Solaris/x86 3.0.35, Solaris/x86 3.0.45, ICA Client for Windows 6.1, 6.20.985, 6.31.1051 | A vulnerability exists when a session is initiated with the server because the server's public key is not validated, which could let a malicious user initiate a man-in-the-middle attack. | No workaround or patch available at time of publishing. | Citrix ICA Client Server Key Verification | Medium | Bug discussed in newsgroups and websites. |
| Compaq[25] | Unix | Tru64 4.0g, 4.0g PK3 (BL17), 4.0f, 4.0f PK7 (BL18), PK6 (BL17), 5.1b, 5.1b PK1 (BL1), 5.1a, 5.1a PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, 5.1 PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17) | A vulnerability exists in 'screend,' which could let a malicious user obtain elevated privileges. | Upgrades available at: http://ftp.support.compaq.com/patches/public/unix/ | Tru64 'screend' Privilege Escalation | Medium | Bug discussed in newsgroups and websites. |
| Copper-mine[26] | Multiple | Photo Gallery 1.0 RC3 | A vulnerability exists due to insufficient sanitization of user-supplied filenames, which could let a remote malicious user execute arbitrary PHP code. | Upgrade available at: http://www.chezgreg.net/coppermine/mod.php?mod=downloads&op=viewdownload&cid=2 | Photo Gallery PHP Code Injection | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[24] SecurityFocus, April 4, 2003.
[25] Hewlett-Packard Company Security Bulletin, April 17, 2003
[26] Bugtraq, April 7, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| eZ Systems[27] | Windows, Unix | eZ publish 3.0, 2.2.7 | Multiple vulnerabilities exist: an information disclosure vulnerability exists because the 'site,ini' configuration file may be downloaded, which could let a remote malicious user obtain sensitive information; several Cross-Site Scripting vulnerabilities exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code; and multiple vulnerabilities exist because scripts under "/kernel/class" and "/kernel/classes" return path information, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | EZ Publish Multiple Vulnerabilities | Medium/ **High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. |
| FileMaker Inc.[28] | Windows NT, 4.0/2000, MacOS 8.0, 8.1, 8.5, 8.6, 9.0, Unix | FileMaker Pro 5.0, 5.5, 5.5 Unlimited, 6.0, 6.0 Unlimited, FileMaker Server 5.0, 5.5 | A vulnerability exists because credentials are not properly secured during authentication, remote malicious user obtain sensitive information and unauthorized access. | Workaround available at: http://www.filemaker.com/ti/108462.html | FileMaker Pro Authentication Disclosure | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| FipsASP[29] | | fipsGuest-book 1.12.7 | A vulnerability exists in the 'new_entry.asp' script due to insufficient sanitization of form data, which could let a remote malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. | FipsGuestbook New_Entry. ASP Arbitrary HTML Injection | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| GNOME [30] | Unix | Balsa 2.0.6, 1.2.4, 1.1.7; libesmtp libesmtp 0.8.9, 0.8.4, 0.8.10p1, 0.8.10 | A buffer overflow vulnerability exists in the read_smtp_response() function, which could let a malicious user execute arbitrary code. | **Gnome:** http://balsa.gnome.org/balsa-2.0.10.tar.bz2 **RedHat:** ftp://updates.redhat.com/ **libesmtp:** http://www.stafford.uklinux.net/libesmtp/libesmtp-1.0.tar.bz2 | libesmtp read_smtp_response Buffer Overflow CVE Name: CAN-2002-1090 | **High** | Bug discussed in newsgroups and websites. |

[27] Security Corporation Security Advisory, SCSA-016, April 15, 2003.
[28] Bugtraq, April 9, 2003.
[29] Black Tigerz Research Group, April 14, 2003.
[30] Red Hat Security Advisory, RHSA-2003:109-03, April 3, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| GNOME [31, 32] | Unix | GtkHTML 1.1.9, 1.1.10 | A Denial of Service vulnerability exists in the GtkHTML library that is distributed with Ximian Evolution when certain malformed messages are submitted. | **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php | GTKHTML Denial of Service CVE Name: CAN-2003-0133 | Low | Bug discussed in newsgroups and websites. |
| gs-common[33] | Unix | gs-common 0.3.3 | A vulnerability exists in the 'ps2espi' script because files are created in an insecure manner when Ghostscript is invoked, which could let a malicious user overwrite files owned by a user who invokes ps2epsi. | Upgrade available at: http://security.debian.org/pool/updates/main/g/gs-common/gs-common_0.3.3.0woody1_all.deb | GS-Common PS2Epsi Insecure Temporary File | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| HTML-Helper [34] | Windows | EZ Server 1.0 | A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | EZ Server Directory Traversal | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Hung-Yih Chen[35] | Unix | ChiTeX 6.1.2p7.8 | A vulnerability exists in two setuid root binaries because they execute the 'cat' program without an absolute path, which could let a malicious user execute arbitrary code with root privileges. | No workaround or patch available at time of publishing. | ChiTeX Path Specification | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| IBM[36] | Unix | AIX 4.3.3, 5.1, 5.2 | An authentication vulnerability exists in the 'secldapclntd' daemon, which could let a remote malicious obtain unauthorized access to data. | Hotfix available at: ftp://aix.software.ibm.com/aix/efixes/security/secldap_efix.tar.Z | AIX 'secldapclntd' Unauthorized Data Access CVE Name: CAN-2003-0119 | Medium | Bug discussed in newsgroups and websites. |
| IBM[37] | Unix | AIX 5.2 | A vulnerability exists when the FTPD implementation and Kerberos 5 are used for authentication, which could let an unauthorized remote malicious user obtain root access. | Patch available at: http://techsupport.services.ibm.com/rs6k/fixes.html | IBM FTP Daemon Administrative Access CVE Name: CAN-2003-0170 | **High** | Bug discussed in newsgroups and websites. |

[31] RedHat Security Advisory, RHSA-2003:126-06, April 15, 2003.
[32] Mandrake Linux Security Update Advisory, MDKSA-2003:046, April 15, 2003.
[33] Debian Security Advisory, DSA 286-1, April 14, 2003.
[34] Security Corporation Security Advisory, SCSA-017, April 17, 2003.
[35] SecurityTracker Alert ID, 106452, April 3, 2003.
[36] SecurityFocus, April 3, 2003.
[37] SecurityTracker Alert ID, 1006455, April 3, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Ikonboard .com[38] | Windows, Unix | IkonBoard 3.1.1 | A vulnerability exists in the LoadLanguage() function due to insufficient sanitization of user-supplied cookie data, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | IkonBoard Load Language() Function | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Internet Software Center[39] | Multiple | Guestbook | A vulnerability exists in the 'gb_eintragen.asp' script file due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Guestbook 'gb_eintragen. asp' Arbitrary Code | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Invision Power Services[40] | Multiple | Invision Board 1.1.1 | An input validation vulnerability exists in the 'functions.php' script file, which could let a malicious user execute arbitrary code. | Patch available at: http://www.invisionboard.com/downloads/patch_apr03.zip | Invision Board functions.php SQL Injection | **High** | Bug discussed in newsgroups and websites. |
| KDE[41, 42, 43] | Unix | KDE 2.0-3.1.1 | A vulnerability exists when specially formatted PDF and PS files are processed due to the way the Ghostscript software is used, which could let a malicious user execute arbitrary commands. | **KDE:** http://download.kde.org/stable/3.0.5b/ **Debian:** http://security.debian.org/pool/updates/main/k/kdegraphics/ | KDE Postscript/PDF File Processing | **High** | Bug discussed in newsgroups and websites. |
| Khaled Mardam-Bey[44] | Windows 95/98/ME/ NT 4.0/2000, XP | mIRC 5.0, 5.1, 5.3-5.91, 6.0- 6.0**.3** | A vulnerability exists in the DCC Get dialog, which could let a remote malicious user spoof a legitimate file. | No workaround or patch available at time of publishing. | MIRC DCC Get Dialog File Spoofing | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Leif M Wright[45] | Windows, Unix | Guestbook 4.0 | An information disclosure vulnerability exists in the 'passwd' file, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Guestbook 'passwd' File Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Leif M Wright[46] | Windows, Unix | Super Guestbook 1.0 | An information disclosure vulnerability exists in the 'superguestconfig' file, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Super Guestbook 'superguest-config' File Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[38] SecurityTracker Alert ID, 1006446, April 2, 2003.
[39] Black Tigerz Research Group Advisory, April 8, 2003.
[40] Bugtraq, April 4, 2003.
[41] KDE Security Advisory, April 9, 2003.
[42] Debian Security Advisory, DSA 284-1, April 12, 2003.
[43] Sorcerer Update Advisory SORCERER2003-04-12, April 12, 2003.
[44] Bugtraq, April 7, 2003.
[45] Secunia Security Advisory, April 14, 2003.
[46] Bugtraq, April 10, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Linksys[47] | Multiple | BEFVP41 1.40 .4, 1.40 .3f | A vulnerability exists because the admin password for the Wireless Access Point is transmitted in plaintext, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | BEFVP41 Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Matriks A/S[48] | Windows 2000 | QuickFront 1.0.0.189 | An information disclosure vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information. | Affected users are advised to contact the vendor for upgrade details. | QuickFront Remote Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Metrics[49] | Unix | Metrics 1.0 | A vulnerability exists because the 'halstead' and 'gather_stats' scripts open temporary files without taking appropriate security precautions, which could let a malicious user corrupt sensitive system files. | Upgrades available at: http://security.debian.org/pool/updates/main/m/metrics/ | Metrics Insecure Local File Creation<br><br>CVE Name: CAN-2003-0202 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| **Microsoft**[50]<br><br>***Microsoft issues bulletin***[51] | **Windows 95/98/ME/ NT 4.0/2000, XP** | **Virtual Machine 3802 Series, 3805 Series, *3809 Series, 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, Terminal Services, SP1-SP3*** | **A vulnerability exists because an applet that is constructed at the bytecode-level may be able to perform some illegal operations, which could let a malicious user bypass security constraints and execute arbitrary code.** | ***Frequently asked questions regarding this vulnerability and the workaround can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-011.asp** | **Microsoft Java Virtual Machine Bytecode Verifier**<br><br>**CVE Name: CAN-2003-0111** | **High** | **Bug discussed in newsgroups and websites.**<br><br>***Exploit scripts have been published.***<br><br>***Vulnerability has appeared in the press and other public media.*** |

[47] Securiteam, April 14, 2003.
[48] SecurityFocus, April 9, 2003.
[49] Debian Security Advisory, DSA 279-1, April 7, 2003.
[50] Bugtraq, November 20, 2002.
[51] Microsoft Security Bulletin, MS03-011, April 14, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft [52] | Windows XP | Windows .NET Datacenter Server Beta 3, Windows .NET Enterprise Server RC2, Beta 3, Windows .NET Standard Server Beta 3, Windows .NET Web Server Beta 3, Windows Server 2003, XP Home, XP Profes-sional | A Denial of Service vulnerability exists in the 'EngTextOut' function if it is passed using non-ASCII characters. | No workaround or patch available at time of publishing. | Windows 'EngTextOut' Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Microsoft [53] | Windows 2000 | Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3 | A vulnerability exists due to the way Domain Controllers manage the Schema and Configuration partitions, which could let a malicious user obtain root access. | No workaround or patch available at time of publishing. | Microsoft Windows Active Directory Policy Bypass | **High** | Bug discussed in newsgroups and websites. |
| Microsoft [54] | Windows 2000 | Internet Explorer 6.0 SP1 | A Denial of Service vulnerability exists due to the way the Object tag is processed when a malicious user submits a page that contains specially crafted HTML. | No workaround or patch available at time of publishing. | Internet Explorer Object Tag Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[52] Bugtraq, April 14, 2003.
[53] NTBugtraq, April 11, 2003.
[54] Bugtraq, April 16, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft [55] | Windows NT 4.0/2000, XP | Windows 2000 Advanced Server, SP1-SP3, 2000 Data-center Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SPa, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1 | A buffer overflow vulnerability exists in the way the kernel passes error messages to a debugger due to insufficient bounds checking, which could let a malicious user take any action on the system including deleting data, adding accounts with administrative access, execute arbitrary code, or reconfiguring the system. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-013.asp | Windows Kernel Message Handling Buffer Overflow<br><br>CVE Name: CAN-2003-0112 | Medium/ **High**<br><br>**(High if adminis-trative access is obtained or arbitrary code can be executed)** | Bug discussed in newsgroups and websites.<br><br>Vulnerability has appeared in the press and other public media. |
| Microsoft [56] | Windows NT 4.0/2000 | ISA Server 2000, 2000 SP1, FP1, Proxy Server 2.0, 2.0 SP1 | A remote Denial of Service vulnerability exists in the Winsock Proxy service because some types of traffic are not handled properly. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-012.asp | Winsock Proxy Service Remote Denial of Service<br><br>CVE Name: CAN-2003-0110 | Low | Bug discussed in newsgroups and websites.<br><br>Vulnerability has appeared in the press and other public media. |

[55] Microsoft Security Bulletin, MS03-013, April 17, 2003.
[56] Microsoft Security Bulletin, MS03-012, April 9, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Mollen-soft Software[57] | Windows 95/98/NT 4.0/2000 | Hyperion FTP Server 3.0 | A buffer overflow vulnerability exists in the FTP 'USER' command due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. | Anyone who is using a version installed before 5/4/03 is advised to download and install the new version available at: http://www.mollensoft.com/product2.htm\ | Hyperion FTP Server USER Command Buffer Overflow | Low/**High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |
| Mollen-soft Software[58] | Windows | Hyperion FTP Server 2.7, 2.8.11, 3.0 | A buffer overflow vulnerability exists due to insufficient bounds checking of FTP 'mkdir' commands, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. | No workaround or patch available at time of publishing. | Hyperion FTP Server MKDIR Buffer Overflow | Low/**High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published. |
| Multiple Vendors[59] | Unix | FreeBSD 4.0-4.7; Linux kernel 2.2-2.2.25, 2.4-2.4.20 | A vulnerability exists when attempting to access existent and non-existent files by examining the amount of time it takes for an error to be returned, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Multiple Vendor I/O System Call File Existence | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published. |

[57] DataSEC Advisory, April 8, 2003.
[58] Tripbit Security Advisory, TA-2003-03, April 4, 2003.
[59] Bugtraq, April 2, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[60] | Unix | Conectiva Linux 3.0-8.0; Debian Linux 2.0-3.0; FreeBSD 5.0 & prior; Mandrake Corporate Server 1.0.1, 2.1, Linux 6.0-9.0, Multi Network Firewall 8.2, Single Network Firewall 7.2; NetBSD 1.0-1.6.1; OpenBSD 2.0-3.2; RedHat Linux 2.0, 2.1, 3.0.3, 4.0-8.0, 9.0 i386; SuSE Linux 4.2-8.2, Linux Admin-CD for Firewall, Connectiv-ity Server, Database Server, Enterprise Server 7, S/390; Slackware Linux 2.0, 2.0.35, 2.1-8.1; Sun Solaris 2.5, _x86, 2.5.1, _x86, ppc, 2.6, sparc, x86, 7.0-9.0, _x86 | A vulnerability exists in the Pluggable Authentication Modules (PAM) through analysis of the response time during authentication, which could let a remote user obtain sensitive information. | No workaround or patch available at time of publishing. | PAM Authentication Timing Information Leakage | Medium | Bug discussed in newsgroups and websites. |

[60] SecurityFocus, April 14, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[61, 62, 63, 64, 65, 66, 67] | MacOS 10.2- 10.2.4; Unix | Compaq Tru64 4.0x, 5.0x; HP HP9000 servers running CIFS/9000 Server versions through A.01.09.02 on HP-UX 11.0, 11.11(11i), and 11.22; Samba Samba 2.0.0-2.0.10, 2.2.0, 2.2.0a, 2.2.1 a, 2.2.3 a-2.2.8, Samba-TNG 0.3, 0.3.1; Sun Solaris 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86, Update 2 | Multiple remote buffer overflow vulnerabilities exist, which could let a remote malicious user execute arbitrary code with root privileges. | **Debian:** http://security.debian.org/pool/updates/main/s/samba/ **Immunix:** http://download.immunix.org/ImmunixOS **Samba:** http://us1.samba.org/samba/ftp/samba-2.2.8a.tar.gz **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **OpenPKG:** ftp://ftp.openpkg.org/release **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/ **RedHat:** ftp://updates.redhat.com/ | Multiple Vendor Samba Unspecified Remote Buffer Overflows<br><br>CVE Name: CAN-2003-0196 | **High** | Bug discussed in newsgroups and websites.<br><br>Vulnerability has appeared in the press and other public media. |

[61] Debian Security Advisory, DSA 280-1, April 7, 2003.
[62] FreeBSD Security Advisory, FreeBSD-SN-03:01, April 7, 2003.
[63] Immunix Secured OS Security Advisory, IMNX-2003-7+-006-01, April 7, 2003.
[64] Mandrake Linux Security Update Advisory, MDKSA-2003:044, April 7, 2003.
[65] OpenPKG Security Advisory, OpenPKG-SA-2003.028, April 7, 2003.
[66] Red Hat Security Advisory, RHSA-2003:137-02, April 9, 2003.
[67] Hewlett-Packard Company Security Bulletin, HPSBUX0304-254, April 9, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79] | MacOS 10.2- 10.2.4; Unix | MacOS X 10.2-10.2.4; Compaq Tru64 4.0x, 5.0x; HP HP9000 servers running CIFS/9000 Server versions through A.01.09.02 on HP-UX 11.0, 11.11(11i), and 11.22; Samba Samba 2.0.0-2.0.10, 2.2.0, 2.2.0a, 2.2.1 a, 2.2.3 a-2.2.8, Samba-TNG 0.3, 0.3.1; Sun Solaris 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86, Update 2 | A buffer overflow vulnerability exists for Samba in the 'call_trans2open' function when user-supplied data is copied into a static buffer, which could let a remote malicious user obtain root access and execute arbitrary commands. | **Apple:** http://docs.info.apple.com/article.html?artnum=120211<br>**Debian:** http://security.debian.org/pool/updates/main/s/samba/<br>**Conectiva:** ftp://atualizacoes.conectiva.com.br<br>**Immunix:** http://download.immunix.org/ImmunixOS<br>**Samba:** http://us1.samba.org/samba/ftp/samba-2.2.8a.tar.gz<br>**Slackware:** ftp://ftp.slackware.com/pub/slackware/<br>**OpenPKG:** ftp://ftp.openpkg.org/release<br>**Mandrake:** http://www.mandrakesecure.net/en/ftp.php<br>**Trustix:** http://www.trustix.net/pub/Trustix/updates/<br>**SGI:** ftp://patches.sgi.com/support/free/security/patches/<br>**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/<br>**RedHat:** ftp://updates.redhat.com/<br>**SuSE:** ftp://ftp.suse.com/pub/suse/ | Multiple Vendors Samba 'call_trans 2open' Remote Buffer Overflow<br><br>CVE Name: CAN-2003-0201 | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published.<br><br>Vulnerability has appeared in the press and other public media. |

[68] Debian Security Advisory, DSA 280-1, April 7, 2003.
[69] FreeBSD Security Advisory, FreeBSD-SN-03:01, April 7, 2003.
[70] Immunix Secured OS Security Advisory, IMNX-2003-7+-006-01, April 7, 2003.
[71] Mandrake Linux Security Update Advisory, MDKSA-2003:044, April 7, 2003.
[72] SuSE Security Announcement, SuSE-SA:2003:025, April 7, 2003.
[73] OpenPKG Security Advisory, OpenPKG-SA-2003.028, April 7, 2003.
[74] Trustix Secure Linux Security Advisory, TSLSA-2003-0019, April 8, 2003.
[75] Conectiva Linux Security Announcement, CLA-2003:624, April 8, 2003.
[76] Red Hat Security Advisory, RHSA-2003:137-02, April 9, 2003.
[77] SGI Security Advisory, 20030403-01-P, April 9, 2003.
[78] Hewlett-Packard Company Security Bulletin, HPSBUX0304-254, April 9, 2003.
[79] Apple Security Update, 61798, April 10, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| nerdlogic.org [80] | Windows | Jpegx 1.0.6 | A vulnerability exists because arbitrary passwords are accepted when decrypting a hidden encrypted message and a weak encryption algorithm is used, which could let a malicious user obtain sensitive information. | Upgrade available at: http://www.nerdlogic.org/cgi-bin/dl2.pl?f=2 | JPEGX Encryption Weakness | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| NetComm [81] | Multiple | NB1300 4.4.1 | A vulnerability exists due to weak default configuration settings, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | NB1300 Weak Default Configuration Settings | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| NetGear[82] | Multiple | FM114P | An information disclosure vulnerability exists if Remote Access and Universal Plug and Play are both enabled on the WAN interface, a UPnP SOAP request can retrieve the username and password, which cold let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | FM114P ProSafe Wireless Router UPnP Information Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| NetGear[83] | Multiple | FM114P | A vulnerability exists if Remote Access and Universal Plug and Play are both enabled on the WAN interface because a UPnP SOAP request can cause a connection to be initiated through a port that is normally blocked, which could let a malicious user bypass security restrictions. | No workaround or patch available at time of publishing. | FM114P ProSafe Wireless Router Rule Bypass | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| NetGear[84] | Multiple | RP114 3.26 | Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to the way the device logs hostnames when content filters are used, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because log requests are not properly handled when content filters are used, which could let a remote malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. | NetGear Router Cross-Site Scripting & Log Requests | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[80] Secunia Security Advisory, April 8, 2003.
[81] Bugtraq, April 15, 2003.
[82] Bugtraq, April 2, 2003.
[83] Bugtraq, April 2, 2003.
[84] SecurityTracker Alert ID, 1006587, April 16, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| NetScreen [85] | Unix | NetScreen-Global PRO Policy Manager Server 4.1.0r1-4.0.0r5 | A vulnerability exists in the Global PRO Policy Manager definitions for IPSec phase 1 and phase 2 proposals using the AES cryptographic algorithms causes VPN configurations in NetScreen firewall/VPN appliances and systems to use the DES encryption which may result in a weaker than intended encryption routines used in IPSec tunnels. | **Workaround:** Users are advised to create custom proposals for IPSec phase 1 and phase 2 using AES128 as the encryption scheme and update all affected VPN configurations to use the newly created proposals. | NetScreen Global PRO Policy Manager IPSec Tunnel Security Configuration | Medium | Bug discussed in newsgroups and websites. |
| Novell[86] | Multiple | Groupwise 6.0, 6.0 SP1&SP2 | Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the Mail Transport Agent (MTA) due to the inclusion of a vulnerable version of OpenSSL; and an information disclosure vulnerability exists in URLS contained in the 'Internet History,' which could let a remote malicious user obtain sensitive information. | GroupWise 6.0 SP3 is not vulnerable and is available at: http://support.novell.com/servlet/filedownload/pub/gw6sp3m.exe | Novell Groupwise Multiple Vulnerabilities | Low/ Medium | Bug discussed in newsgroups and websites. There is no exploit code required for the information disclosure vulnerability. |
| Ocean12 Technol-ogies[87] | Windows | ASP Guestbook Manager 1.0 | Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'add.asp' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the MS Access database can be downloaded, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | ASP Guestbook Manager Cross-Site Scripting & Information Disclosure | Medium/ **High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. There is no exploit code required for the Cross-Site Scripting vulnerability. Proof of Concept exploit has been published for the information disclosure vulnerability. |
| OpenSSH [88] | Unix | OpenSSH 2.2, 2.3, 2.5-2.5.2, 2.9, 2.9 p1&2, 2.9.9, 3.0, 3.0p1, 3.0.1, 3.0.1p1, 3.0.2 | A vulnerability exists through analysis of the response time during authentication, which could let a remote user obtain sensitive information. | No workaround or patch available at time of publishing. | OpenSSH Authentication Execution Path Timing Information Leakage | Medium | Bug discussed in newsgroups and websites. |

[85] NetScreen Security Advisory, 57226, April 16, 2003.
[86] Secunia Security Advisory, April 16, 2003.
[87] Black Tigerz Research Group Advisory, April 11, 2003.
[88] SecurityFocus, April 14, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Opera Software[89] | Windows 95/98/ME/ NT 4.0/2000, XP | Opera Web Browser 6.0.1 win32 | A vulnerability exists because potentially dangerous Java methods can be called with JavaScript, which could let a malicious user execute arbitrary commands. | Vulnerability does not appear to be present in Opera 7.02 for Windows. Upgrading to this version may address the issue, though this has not been confirmed. | Opera JavaScript Java Method Access | **High** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. |
| Oracle Corpora-tion[90] | Windows NT 4.0/2000, Unix | Oracle Applica-tions 10.7, 11.0, E-Business Suite 10.7, 11.0, E-Business Suite 11i 11.1-11.8 | A vulnerability exists in the communications protocol used by the FND File Server (FNDFS) program, which could let a remote malicious user bypass operating system, database, and application authentication mechanisms to retrieve arbitrary files from Oracle Applications Concurrent Manager servers. | Patches available at: http://metalink.oracle.com | Oracle E-Business Suite RRA/FNDFS File Disclosure | Medium | Bug discussed in newsgroups and websites. |
| Orplex Consult-ing, Inc.[91] | Windows | Guest Book | A vulnerability exists in the 'addentry.asp' script due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Guest Book 'Addentry.asp' Code Injection | **High** | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| osCom-merce[92] | Windows, Unix | osCom-merce 2.2 cvs | A remote Denial of Service vulnerability exists when malicious URI parameters are passed to several PHP pages. | No workaround or patch available at time of publishing. | OSCommerce Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| osCom-merce[93] | Windows, Unix | osCom-merce 2.2 cvs | A vulnerability exists because HTTP header information is used as part of the authentication mechanism, which could let a malicious user spoof parts of the HTTP header and bypass authentication. | No workaround or patch available at time of publishing. | OSCommerce Authentication Bypass | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[89] Bugtraq, April 2, 2003.
[90] Integrigy Security Advisory, April 10, 2003.
[91] Black Tigerz Research Group, April 7, 2003.
[92] SecurityFocus, April 15, 2003.
[93] SecurityFocus, April 15, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Paul Sheer[94] | Unix | SheerDNS 1.0 | Multiple vulnerabilities exist: a buffer overflow vulnerability exists when responses are constructed to CNAME queries due to insufficient bounds checking of lookup information, which could let a malicious user cause a Denial of Service or execute arbitrary code; and a Directory Traversal vulnerability exists in directory_lookup() due to insufficient sanitization of DNS requests, which could let a malicious user obtain sensitive information. | Upgrade available at: http://threading.2038bug.com/sheerdns/sheerdns-1.0.1.tar.gz | SheerDNS Buffer Overflow & Directory Traversal | Low/ Medium/ **High** **(Low if a DoS; Medium if sensitive informa-tion can be obtained; and High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published for the Directory Traversal vulnerability. |
| Phorum. org [95] | Windows, Unix | Phorum 3.2.4-3.2.8, 3.3.1 a, 3.3.1, 3.3.2 a, 3.3.2b3, 3.3.2, 3.4 | A Cross-Site Scripting vulnerability exists due to insufficient filtering of user-supplied HTML code from the 'title' field, which could let a remote malicious user execute arbitrary code. | Upgrade available at: http://phorum.org/downloads/phorum-3.4.2.tar.gz | Phorum Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| phPay[96] | Windows, Unix | phPay 2.2 | Multiple vulnerabilities exist: several path disclosure vulnerabilities exist when specially crafted requests are made for many phPay pages and include files, which could let a malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists in the 'search.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and an information disclosure vulnerability exists due to insufficient authentication when viewing administration pages, which could let a malicious user obtain sensitive information. | Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=39285 | PHPay Multiple Path Disclosure & Cross-Site Scripting Vulnerabilities | Medium/ **High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. There is no exploit code required for the information disclosure vulnerability. |

[94] Bugtraq, April 13, 2003.
[95] Secunia Security Advisory, April 3, 2003.
[96] ALPER Research Labs Security Advisory, ARL03-A16, April 9, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| phpSys Info[97] | Unix | phpSysInfo 2.1 | A file disclosure vulnerability exists because the include path for several template files and language include files can be influenced, which could let a malicious user obtain sensitive information and execute arbitrary code. | No workaround or patch available at time of publishing. | PHPSysInfo File Disclosures | Medium/ **High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Pleasure Net Consult-ing Inc.[98] | Windows, Unix | InstaBoard 1.3 | Multiple input validation vulnerabilities exist in the 'index.cfm' file, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | InstaBoard Index.CFM Input Validation | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| PoPToP[99] | Unix | PPTP Server 1.0.1, 1.1.2-1.1.4-b2 | A buffer overflow vulnerability exists due to insufficient sanity checks when referencing user-supplied input used in various calculations, which could let a remote malicious user execute arbitrary code | Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=44827 | PoPToP PPTP Remote Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Progress Software Corpora-tion[100] | Unix | Progress Database 8.3V, 8.3E, 8.3D, 9.1D, 9.1C, 9.1B | A vulnerability exists because configuration files are read as the root user without verifying that the user has permission to read the configuration files, which could let a malicious user obtain elevated privileges and sensitive information. | No workaround or patch available at time of publishing. | Progress Database Configuration File Verification | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Progress Software Corpora-tion[101] | Windows NT 4.0/2000, Unix | Database 8.3V, 8.3E, 8.3 D, 9.1B-9.1 D | A buffer overflow vulnerability exists in the 'DLC' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code as root. | Upgrades available at: http://www.progress.com/patches/ | Progress Database DLC Environment Variable | **High** | Bug discussed in newsgroups and websites. |
| Progress Software Corpora-tion[102] | Windows NT 4.0/2000, Unix | Database 9.1 D | A buffer overflow vulnerability exists in the 'BINPATHX' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code. | Upgrade available at: http://www.progress.com/patches/ | Progress Database 'BINPATHX' Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Py-Membres [103] | Windows | Py-Membres 4.0 | A vulnerability exists in the 'login.php' file, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Py-Membres Remote SQL Injection | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[97] SecurityFocus, April 4, 2003.
[98] Bugtraq, April 14, 2003.
[99] Bugtraq, April 9, 2003.
[100] Secure Network Operations, Inc. Advisory, SRT2003-04-02-1735, April 2, 2003.
[101] Secure Network Operations, Inc. Advisory, SRT2003-04-15-1029, April 9, 2003.
[102] Secure Network Operations, Inc., SRT2003-04-15-1029, April 15, 2003.
[103] SecurityFocus, April 7, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Python Software Founda-tion[104] | Unix | Python 2.2.2, 2.3 | A Cross-Site Scripting vulnerability exists in the error pages, which could let a remote malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. | Python Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Sakki[105] | Windows | Guestbook 1.01 | A vulnerability exists in 'gb.asp' due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Guestbook HTML Injection | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| SETI[106] | Multiple | SETI@ home 3.03-3.07 | Several vulnerabilities exist: a vulnerability exists in the client program because information is transmitted from the client to the server in plaintext, which could let a malicious user obtain sensitive information; and a vulnerability exists in the client program due to insufficient bounds checking when processing server data, which could let a malicious user execute arbitrary commands. | Upgrade available at: http://setiathome.ssl.berkeley.edu/download.html | SETI@home Client Program Multiple Vulnerabilities | Medium/ **High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. There is no exploit code required for the plain text vulnerability. Vulnerability has appeared in the press and other public media. |
| SGI[107, 108, 109] | Unix | SGI IRIX 6.5-6.5.19, 6.5m-6.5.19m, 6.5f-6.5.19f; xfsdump xfsdump 2.0.0-2.0.5, | A vulnerability exists in 'xfsdump' because quota information files are handled insecurely, which could let a malicious user obtain elevated privileges. | **SGI:** ftp://patches.sgi.com/support/free/security/patches/ **Debian:** http://security.debian.org/pool/updates/main/x/xfsdump/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php | XFSDump Quotas File CVE Name: CAN-2003-0173 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| SmartMax Software [110] | Windows NT 4.0/2000, XP | MailMax 5.0.10.7, 5.0.10.6, 5.0 | A buffer overflow vulnerability exists when a specially crafted password argument is used for the IMAP Login command, which could let a remote malicious user cause a Denial of Service and execute arbitrary code with system privileges. | Updated replacement files available at: ftp://ftp.smartmax.com/updates/MailMax5.0/ | MailMax Password Field Buffer Overflow | Low/**High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[104] Secunia Security Advisory, April 4, 2003.
[105] Bugtraq, April 3, 2003
[106] SecurityFocus, April 12, 2003.
[107] SGI Security Advisory, 20030404-01-P, April 10, 2003.
[108] Debian Security Advisory, DSA 283-1, April 11, 2003.
[109] Mandrake Linux Security Update Advisory, MDKSA-2003:047, April 16, 2003.
[110] Secunia Security Advisory, April 14, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Snitz Communications[111] | Windows, Unix | Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3 | A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied <IMG> tags, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Snitz Forums 2000 Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| **Snort Project[112, 113, 114]**<br><br>***More upgrades issued[115]*** | **Unix** | **Snort 1.8-1.8.7, 1.9** | **A buffer overflow vulnerability exists in the network IDS due to a flaw in the RPC preprocessor, which could let a remote malicious execute arbitrary instructions with root privileges.** | **Upgrade available at:** **http://www.snort.org/dl/snort-1.9.1.tar.gz**<br>**Mandrake:** **http://www.mandrakesecure.net/en/ftp.php**<br>**EnGarde:** **http://ftp.engardelinux.org/pub/engarde/stable/updates/**<br>**SmoothWall:** **http://www.smoothwall.org/get/download/patches/1.0-20030304-fixes2.html**<br><br>***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** | **Snort RPC Preprocessor Fragment Reassembly Buffer Overflow**<br><br>**CVE Name: CAN-2003-0033** | **High** | **Bug discussed in newsgroups and websites.** |
| Snort Project[116, 117] | Unix | Snort 1.8-1.8.7, 1.9, 1.9.1; Smooth Wall 2.0 beta 4 | A buffer overflow vulnerability exists during the reassembly of TCP packets by the stream4 preprocesser, which could let a remote malicious user execute arbitrary code. | **Snort Project:** http://www.snort.org/dl/snort-2.0.0.tar.gz<br>**SmoothWall:** http://us0.download.smoothwall.org/archive/updates/2.0/b4/2.0b4-mallard-fixes2.tar.gz | Snort TCP Packet Reassembly Buffer Overflow<br><br>CVE Name: CAN-2003-0029 | High | Bug discussed in newsgroups and websites. |
| Thomas Boutell[118] | Multiple | cgic 2.0, 2.0.1 | A buffer overflow vulnerability exists due to insufficient bounds checking of client-supplied cookie header data, which could corrupt sensitive regions of memory on a host. | Upgrade available at: http://www.boutell.com/cgic/cgic202.tar.gz | CGIC CGICookie String Buffer Overflow | Medium | Bug discussed in newsgroups and websites. |

[111] Bugtraq, April 17, 2003.
[112] DHS/IAIP Advisory 03-003, March 3, 2003.
[113] Mandrake Linux Security Update Advisory, MDKSA-2003:029, March 6, 2003.
[114] EnGarde Secure Linux Security Advisory, ESA-20030307-007, March 7, 2003.
[115] Conectiva Linux Security Announcement, CLA-2003:613, April 4, 2003.
[116] NIPC/DHS Advisory 03-018, April 17, 2003.
[117] CERT Advisory, CA-2003-13, April 17, 2003.
[118] SecurityFocus, April 16, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Twilight Utilities[119] | Windows 2000, XP | TW_Web Server 1.0 | A remote Denial of Service vulnerability exists when a malicious user submits an excessive amount of data as part of a HTTP GET request. Execution of arbitrary code may also be possible. | No workaround or patch available at time of publishing. | TW-Web Server Denial of Service | Low/**High**<br><br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.<br><br>Vulnerability has appeared in the press and other public media. |
| Vignette [120] | Windows, Unix | StoryServer 4.1, 6.0 | A vulnerability exists in the TCL interpreter when generating dynamic pages, which could let a malicious user obtain sensitive information. | Patch available at: http://support.vignette.com/VOLSS/KB/View/1,,5360,00.html | StoryServer Information Disclosure<br><br>CVE Name: CAN-2002-0385 | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Web Wiz Guide[121] | Windows | Forum 6.34, 7.0 beta1, 7.0 | An information disclosure vulnerability exists in the 'admin/wwforum.mdb' file, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Web Wiz Forum Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Web Wiz Guide[122] | Windows | Site News 3.6 | An information disclosure vulnerability exists in 'news.mdb' because administration credentials are stored in plaintext, which could let a malicious user obtain administrative privileges. | No workaround or patch available at time of publishing. | Web Wiz Site News Information Disclosure | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Xonic.ru [123] | Unix | News 1.0 | A vulnerability exists the 'script.php' file due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | News script.php Remote Command Execution | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Xoops[124] | Windows, Unix | Xoops 1.3.8, 1.3.9 | A Cross-Site Scripting vulnerability exists in the 'glossaire-aff.php' script due to a lack of sanitization on user-supplied input, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Xoops 'glossaire-aff.php' Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

*"Risk" is defined by CyberNotes in the following manner:

[119] SP Research Labs Advisory x02, April 15, 2003.
[120] @stake, Inc. Security Advisory, a040703-1, April 7, 2003.
[121] SecurityTracker Alert ID, 1006597, April 17, 2003.
[122] Black Tigerz Research Group, April 14, 2003.
[123] SecurityFocus, April 16, 2003.
[124] SecurityTracker Alert ID, 1006432, April 1, 2003.

**High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

**Medium** – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

**Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 3 and April 18, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 32 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| April 18, 2003 | 0x82-Remote.54aab4.Xpl.c | Script that exploits the Samba 'call_trans 2open' Remote Buffer Overflow vulnerability. |
| April 18, 2003 | Core-2003-0307.txt | Information on exploiting the Snort TCP Packet Reassembly Buffer Overflow |
| April 18, 2003 | Lkl-0.0.2.tar.gz | A userspace keylogger that runs under Linux x86/arch and logs everything that passes through the hardware keyboard port and supports keycode to ASCII translation. |
| April 18, 2003 | Nessus-2.0.4.tar.gz | A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks. |
| April 18, 2003 | Sormail.c | Exploit script that exploits the Sendmail Address Prescan Buffer Overflow vulnerability. |
| April 18, 2003 | Wellenreiter-v1.8.tar.gz | A GTK/Perl wireless network discovery and auditing tool that has a scanner window which can be used to discover access-points, networks, and ad-hoc cards. It detects essid broadcasting or non-broadcasting networks and detects WEP capabilities and the manufacturer automatically. |
| April 15, 2003 | 0x333xes.c | A simple utility that generates source code for stack overflow exploits. |
| April 15, 2003 | Clicktag.txt | Exploit for the Macromedia Flash Cross-Site Scripting vulnerability. |
| **April 15, 2003** | **Sp-urfuqed.pl** | **Perl script that exploits the TW-Web Server Denial of Service vulnerability.** |
| **April 14, 2003** | **Chindi-dos-poc.c** | **Script that exploits the Chindi Remote Denial of Service vulnerability.** |

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| April 13, 2003 | Dnsfake.c | Script that exploits the SheerDNS Directory Traversal vulnerability. |
| April 10, 2003 | Myptrace.c | Local root exploit for the Linux 2.2 and 2.4 kernels that have a flaw in ptrace where a kernel thread is created insecurely. This version escalates user privileges to root without the necessity of needing access to /proc. |
| April 9, 2003 | 0x82-Remote.Xxxxbsd_Passlogd.Xpl.c | Script that exploits the Passlog Daemon SL_Parse Remote Buffer Overflow vulnerability. |
| April 9, 2003 | Coppermine.tgz | Script that exploits the Photo Gallery PHP Code Injection vulnerability. |
| April 9, 2003 | Fata_jack.c | This tool highlights poor AP security and works by sending authentication requests to an AP with an inappropriate authentication algorithm and status code that causes most makes to drop the relevant associated session. |
| April 9, 2003 | Flawfinder-1.22.tar.gz | Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first. |
| April 9, 2003 | Hl-headnut.c | Denial of service exploit against Half-life servers. |
| April 9, 2003 | Nmbping.pl | Utility for finding Samba and Windows Netbios services that is UDP based and very quick. |
| April 9, 2003 | Sambal.c | Script that exploits the Samba 'call_trans 2open' Remote Buffer Overflow vulnerability. |
| April 7, 2003 | Samba_exp2.tar.gz | Script that exploits the Samba 'call_trans 2open' Remote Buffer Overflow vulnerability. |
| April 7, 2003 | Trans2root.pl | Script that exploits the Samba 'call_trans 2open' Remote Buffer Overflow vulnerability. |
| April 7, 2003 | Verifier_msie401.tar.gz | Script that exploits the Microsoft Java Virtual Machine Bytecode Verifier vulnerability. |
| April 7, 2003 | Verifier_msie45.tar.gz | Script that exploits the Microsoft Java Virtual Machine Bytecode Verifier vulnerability. |
| April 7, 2003 | Verifier_msie456.tar.gz | Script that exploits the Microsoft Java Virtual Machine Bytecode Verifier vulnerability. |
| April 5, 2003 | Regexploit.c | Local exploit/Trojan that makes use of REGEDIT.EXE. Any file containing a value of more than 260 characters causes an error exception by the RegSetValueExW function, which then uses a function of NTDLL.DLL that is vulnerable. |
| April 5, 2003 | Stegtunnel-0.2.tar.gz | A tool written to hide data within TCP/IP header fields that was designed to be undetectable, even by people familiar with the tool. It can hide the data underneath real TCP connections, using real, unmodified clients and servers to provide the TCP conversation |
| April 5, 2003 | Udpremotecontrols.txt | This paper illustrates how to control the server with the UDP protocol. It covers UDP basics, how to spoof datagrams, and gives full source code with explanations. |
| April 5, 2003 | Xlock-XLOCALEDIR.c | Script that exploit the XFree86 XLOCALEDIR overflow vulnerability. |
| **April 4, 2003** | **Filetest.c** | **Script that exploits the Multiple Vendor I/O System Call File Existence vulnerability.** |
| **April 4, 2003** | **Hyperion.c** | **Script that exploits the Hyperion FTP Server MKDIR Buffer Overflow vulnerability.** |
| April 3, 2003 | 0x82-Remote_Passlogd_Sniff_Xpl.C | Script that exploits the Passlog Daemon SL_Parse Remote Buffer Overflow vulnerability. |

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| April 3, 2003 | Nessus-2.0.3.tar.gz | A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks. |

# Trends

- **The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table and DHS/IAIP Advisory 03-018, located at: http://www.nipc.gov/warnings/advisories/2003/03-018.htm**
- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**
- Over the past few weeks, their have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: http://www.cert.org/advisories/CA-2003-08.html.
- **The Department of Homeland Security (DHS), National Infrastructure Protection Center (NIPC) has issued an advisory to heighten awareness of the recently discovered Remote SendMail Header Processing Vulnerability (CAN-2002-1337). NIPC has been working closely with the industry on vulnerability awareness and information dissemination. For more information, see 'Bugs, Holes & Patches' table and DHS/NIPC Advisory 03-004 located at: http://www.nipc.gov/warnings/advisories/2003/03-004.htm. *Note: SendMail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many SendMail servers are not typically shielded by perimeter defense applications.* Remote malicious users may gain access to other systems through a compromised SendMail server, depending on local configurations.**

# Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

**BAT.Excessive.Worm (Batch File Worm):** This is a simple batch file worm that spreads mainly through the KaZaA file-sharing network. It displays various messages containing offensive content. When BAT.Excessive.Worm is executed, it opens several Internet Explorer windows to different adult Web sites and creates numerous copies of itself in many folders on the C drive. It creates about 100 subfolders in the current folder and creates the files:

- C:\Bih.vbs
- C:\Sis.vbs
- C:\End.vbs

Several dialog boxes that contain offensive messages are also displayed.

**Busan (Alias: Win32.Busan) (Win32 Worm):** This worm spreads by copying itself to all accessible network resources. The worm is Windows application (C++ PE EXE-file). It is packed by UPX and is around 14kB large. When executed, the worm sends a message through ICQ to the author of the worm, then copies itself to Windows directory with name "files32.sys," and also copies a file "mh32.dll" there. This is a keyboard hooker that tries to copy itself with the name "auto.exe" to following directory:

- C:\WINDOWS\All Users\Start Menu\Program Files\StartUp\

Because of a bug, this fails. Next the worm copies itself to all accessible network shares. After that the worm registers itself in the system register in a key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command @="files32.sys \"%1\" %*"

This means that when executing any EXE-file the worm will be started. The worm collects information from the local system and tries to send them to the worm writer. This includes addresses, passwords, and results of the keyboard snooper. The worm tries download a file "worm31.bmp" from a web-site in the Internet, but this page has been removed and the download fails.

**W32.HLLW.Gaobot.P (Win32 Worm):** This is a worm that attempts to spread itself to the network shares. This threat also allows for a malicious user to remotely access an infected computer through IRC. It is compressed with UPX.

**W32.HLLW.Morb@mm (Alias: W32/Morb@MM, Morbex, I-Worm.Morbex) (Win32 Worm):** This is a MAPI worm that replies to all the messages in your E-mail Inbox folder and drops the Backdoor.Sdbot Trojan into the infected system. This worm also attempts to spread itself through the KaZaA file-sharing network. The e-mail has the following characteristics:

- Subjects/Message: The subject line and message body is randomly chosen from a list that the worm carries.
- Attachment: Attachment is one of various exe files.

This threat is written in the Bollard Delphi programming language.

**W32.HLLW.Purol (Win32 Worm):** This is a worm that attempts to spread through file-sharing networks and to delete certain files from the infected computer. The worm uses a Zip icon to attempt to disguise itself as an ordinary zip file. W32.HLLW.Purol is written in Microsoft Visual Basic (VB) and compressed with UPX. The VB run-time libraries must be installed for it to execute.

**W32.HLLW.Shydy (Win32 Worm):** This is a worm that attempts to spread through the KaZaA file-sharing network. The worm is written in Microsoft Visual Basic, version 6, and is packed with UPX. The VB run-time libraries must be installed for it to execute.

**W32.Kwbot.F.Worm (Alias: Worm.P2P.SdDrop.d) (Win32 Worm):** This is a worm that attempts to spread across file-sharing networks, such as KaZaA and iMesh. It drops and runs Backdoor.Sdbot and is packed with ASPack v2.12.

**W32/Refoav (Aliases: I-Worm.Refoav, W32.Refoav@mm) (Win32 Worm):** This is a worm that will send itself to contacts found in the Outlook address book. It arrives in an e-mail with the following characteristics:

- Subject line: Fw: Impresionante
- Attached file: foavre.exe

W32/Refoav-A will copy itself to C:\FOAVRE.exe and create the VBScript file C:\vbseli.vbs. This VBScript is not viral and can be deleted. It will create the following registry entry to ensure that vbseli.vbs is run on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Load = C:\vbseli.vbs

When vbseli.vbs is executed, a message will be displayed and it will delete the files C:\FOAVRE.exe and C:\vbseli.vbs. The worm will also store all the e-mail addresses in a file named C:\datospc.dat and then send this file to the malicious user. The file datospc.dat will be deleted on successful completion of this action.

**W95.Tenrobot (Word 95 Macro Virus):** This is a memory-resident file appender that only infects files when it is executed on a Windows 95/98/ME system. It gives a malicious user remote access to your computer through IRC.

**WM97/Kingpawn-A (Word 97 Macro Virus):** This is a macro virus generated from a kit. If you have mIRC, the virus drops a SCRIPT.INI file infected with mIRC/Simp-Fam. If you have pIRCH, WM97/Kingpawn-A will drop an EVENTS.INI file infected with pIRC/Pirch-Fam. If you have vIRC32, the virus will edit the following registry entry by setting Event17 to send out the currently infected document:

- HKCU\Software\MeGALiTH Software\Visual IRC96\Events

WM97/Kingpawn-A will also set an editing password on documents of 'IAMAPORNKING.'

**WORM_AGOBOT.E (Aliases: W32/Gaobot.worm, W32.HLLW.Gaobot, W32/Agobot.B (exact), Worm.P2P.Agobot.b, Win32/HLLW.Agobot.B) (Win32 Worm):** This worm propagates via the KaZaA peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be used to launch a Denial of Service attack against other users. This worm is designed to have backdoor server capabilities that allow remote users to access and manipulate infected systems. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

**WORM_HORSMAN.A (Aliases: W32/Fourseman@MM, I-Worm.Centar.a, Win32/Fohoma.A@mm, Win32.Centar worm, W32.Fourseman.A) (Win32 Worm):** This worm propagates via e-mail using Microsoft Outlook and Internet Relay Chat using mIRC. It is also capable of terminating antivirus and firewall applications. The e-mail that it sends out has the following details:

- Subject: Very important patch!
- Attachment: One of the following:
  - SProcess.exe
  - Great_Virus_Creation_Kit.exe
  - Win_Security_Patch_2602.exe

To propagate via Internet Relay Chat, it modifies the mIRC initialization file, SCRIPT.INI, such that its copy is sent to all users who are in the same IRC channel as the infected user. It also overwrites the system file, EXPLORER.EXE, with a copy of itself to enable its automatic execution at system startup and subsequently gain memory-residency. It is written in Microsoft Visual Basic 6.0, a high-level programming language and usually arrives as a UPX-compressed file.

**Worm/Mickl (P2P Worm):** This is a Peer-2-Peer Internet worm that spreads through many of the popular file-sharing programs such as KaZaA, eDonkey2000, Bearshare, Morpheus, limeWire, Gnucleus, as well as, spreading through the instant messaging software ICQ. If executed, the worm copies itself to "C:\Windows\winstart32.exe" and will copy all *.INI files from within the 'C:\Windows\' to 'C:\Windows\MyShares\.' This folder will be shared in KaZaA, KaZaA lite, Grokster and iMesh. Additionally, it will create the new file, "C:\Windows\MyShares\Readme.txt." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices "Winstart"="C:\\windows\\winstart32.exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Winstart"="C:\\windows\\winstart32.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "HWINFO_BKP"="C:\\windows\\HWINFO_BKP.com"

Additionally, the following keys get added so that it can spread through the use of most file sharing programs:

- HKEY_CURRENT_USER\Software\iMesh\Client\LocalContent "dir0"="012345:C:\\windows\\MyShares"
- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "dir1"="012345:C:\\windows\\MyShares" "dir2"="012345:C:\\windows\\MyShares"
- HKEY_CURRENT_USER\Software\Grokster\LocalContent "dir0"="012345:C:\\windows\\MyShares"

- HKEY_CURRENT_USER\Software\Kazaa lite\LocalContent "dir0"="012345:C:\\windows\\MyShares"

The key HKEY_CURRENT_USER\Software\Lorup also gets created.

**Worm/Yoyks.A (Alias: W32/Yoyks.A) (Win32 Worm):** This is an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book. The worm arrives through e-mail in the following format:

- Subject: Request Information
- Attachment: YOY.exe

The worm copies itself in the following locations:

- C:\Windows\Yoy.exe

It will add the following new files:

- C:\News.bat
- C:\Windows\Yoyks.txt
- C:\Windows\System32\News.htm

If executed, the file NEWS.BAT will create the registry run key so that the worm gets run each time the system is restarted:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "winpif"="c:\\windows\\invir.exe"

It will then change the Start Page of Microsoft Internet Explorer to point to NEWS.HTM:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Start Page"="c:\\windows\\system32\\news.htm"

Anytime Internet Explorer is opened NEWS.HTM is displayed. Within this file is a Visual Basic Script that allows the worm to send itself out via e-mail with Microsoft Outlook to all the e-mail addresses stored in the Windows address book (WAB).

**XM97/Baris-AG (Aliases: X97M_BARISADA.B, X97M.Barisada.Var, X97M/Barisada.gen, Macro.Excel97.Barisada) (Excel 97 Macro Virus):** This is a macro virus. The viral macros are stored in the file book.xls. On 24 April between 2pm and 3pm, the virus displays a series of dialog boxes asking the user questions which may be related to a fantasy role playing game. The first dialog box has the title '1st Qusetion' and the text 'Question: What is the Sword Which Karl Styner(=Grey Scavenger) used?Answer: Barisada.' If the user presses 'No' a message box with the title 'Right Answer' and the message 'Good! You're Authorized now!!' is displayed. If the user presses 'yes' then a message box with the title 'Wrong Answer' and the text 'I will give you one more Chance. Be careful!!' is displayed. The next dialog box has the title 'Wrong Answer may cause The Serious Problem!' and the text 'Summoning Xavier is the Ultimate Magic. Right?.' If the user presses 'Yes' a message box with the title 'Right Answer' and the message 'OK , I will forgive you' appears. If the user presses 'No' a message box with the title 'You shall Die' and the message 'Wrong Answer, Your file will be deleted!' appears. The virus then clears all the cells in all the open sheets.

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| AdwareDropper-A | A | CyberNotes-2003-04 |
| AIM-Canbot | N/A | CyberNotes-2003-07 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| **AprilNice** | **N/A** | **Current Issue** |
| Backdoor.Acidoor | N/A | CyberNotes-2003-05 |
| Backdoor.Amitis | N/A | CyberNotes-2003-01 |
| Backdoor.Assasin.D | D | CyberNotes-2003-01 |
| Backdoor.Assasin.E | E | CyberNotes-2003-04 |
| Backdoor.Beasty | N/A | CyberNotes-2003-02 |
| Backdoor.Beasty.B | B | CyberNotes-2003-03 |
| Backdoor.Beasty.C | C | CyberNotes-2003-05 |
| Backdoor.Beasty.D | D | CyberNotes-2003-06 |
| Backdoor.Beasty.E | E | CyberNotes-2003-06 |
| Backdoor.Bmbot | N/A | CyberNotes-2003-04 |
| Backdoor.Bridco | N/A | CyberNotes-2003-06 |
| Backdoor.CHCP | N/A | CyberNotes-2003-03 |
| Backdoor.Colfuser | N/A | CyberNotes-2003-01 |
| Backdoor.Cow | N/A | CyberNotes-2003-01 |
| Backdoor.Cybspy | N/A | CyberNotes-2003-01 |
| Backdoor.Dani | N/A | CyberNotes-2003-04 |
| Backdoor.Darmenu | N/A | CyberNotes-2003-05 |
| Backdoor.Deftcode | N/A | CyberNotes-2003-01 |
| Backdoor.Delf.F | F | CyberNotes-2003-07 |
| Backdoor.Drator | N/A | CyberNotes-2003-01 |
| Backdoor.Dvldr | N/A | CyberNotes-2003-06 |
| **Backdoor.EggDrop** | **N/A** | **Current Issue** |
| Backdoor.Fluxay | N/A | CyberNotes-2003-07 |
| Backdoor.FTP.Casus | N/A | CyberNotes-2003-02 |
| Backdoor.FTP_Ana.C | C | CyberNotes-2003-07 |
| **Backdoor.FTP_Ana.D** | **D** | **Current Issue** |
| Backdoor.Graybird | N/A | CyberNotes-2003-07 |
| **Backdoor.Graybird.B** | **B** | **Current Issue** |
| **Backdoor.Graybird.C** | **C** | **Current Issue** |
| Backdoor.HackDefender | N/A | CyberNotes-2003-06 |
| Backdoor.Hethat | N/A | CyberNotes-2003-01 |
| Backdoor.Hipo | N/A | CyberNotes-2003-04 |
| Backdoor.Hitcap | N/A | CyberNotes-2003-04 |
| Backdoor.Hornet | N/A | CyberNotes-2003-01 |
| Backdoor.IRC.Aladinz | N/A | CyberNotes-2003-02 |
| Backdoor.IRC.Cloner | N/A | CyberNotes-2003-04 |
| Backdoor.IRC.Yoink | N/A | CyberNotes-2003-05 |
| Backdoor.IRC.Zcrew | N/A | CyberNotes-2003-04 |
| Backdoor.Khaos | N/A | CyberNotes-2003-04 |
| Backdoor.Kilo | N/A | CyberNotes-2003-04 |
| Backdoor.Kol | N/A | CyberNotes-2003-06 |
| Backdoor.Krei | N/A | CyberNotes-2003-03 |
| Backdoor.Lala | N/A | CyberNotes-2003-01 |
| Backdoor.LittleWitch.C | C | CyberNotes-2003-06 |
| Backdoor.Longnu | N/A | CyberNotes-2003-06 |
| Backdoor.Marotob | N/A | CyberNotes-2003-06 |
| Backdoor.Massaker | N/A | CyberNotes-2003-02 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| **Backdoor.Monator** | **N/A** | **Current Issue** |
| Backdoor.MSNCorrupt | N/A | CyberNotes-2003-06 |
| Backdoor.NetDevil.B | B | CyberNotes-2003-01 |
| Backdoor.NetTrojan | N/A | CyberNotes-2003-01 |
| Backdoor.Ohpass | N/A | CyberNotes-2003-01 |
| Backdoor.OICQSer.165 | N/A | CyberNotes-2003-01 |
| Backdoor.OICQSer.17 | 17 | CyberNotes-2003-01 |
| Backdoor.Optix.04.d | 04.d | CyberNotes-2003-04 |
| Backdoor.OptixDDoS | N/A | CyberNotes-2003-07 |
| Backdoor.OptixPro.10.c | 10.c | CyberNotes-2003-01 |
| Backdoor.OptixPro.12.b | 12.b | CyberNotes-2003-07 |
| Backdoor.Plux | N/A | CyberNotes-2003-05 |
| Backdoor.PSpider.310 | 310 | CyberNotes-2003-05 |
| Backdoor.Queen | N/A | CyberNotes-2003-06 |
| Backdoor.Redkod | N/A | CyberNotes-2003-05 |
| Backdoor.Remohak.16 | 16 | CyberNotes-2003-01 |
| Backdoor.RemoteSOB | N/A | CyberNotes-2003-01 |
| Backdoor.Rephlex | N/A | CyberNotes-2003-01 |
| Backdoor.Rsbot | N/A | CyberNotes-2003-07 |
| Backdoor.SchoolBus.B | B | CyberNotes-2003-04 |
| Backdoor.Sdbot.C | C | CyberNotes-2003-02 |
| Backdoor.Sdbot.D | D | CyberNotes-2003-03 |
| Backdoor.Sdbot.E | E | CyberNotes-2003-06 |
| Backdoor.Sdbot.F | F | CyberNotes-2003-07 |
| **Backdoor.Sdbot.G** | **G** | **Current Issue** |
| Backdoor.Serpa | N/A | CyberNotes-2003-03 |
| Backdoor.Servsax | N/A | CyberNotes-2003-01 |
| Backdoor.SilverFTP | N/A | CyberNotes-2003-04 |
| Backdoor.Sixca | N/A | CyberNotes-2003-01 |
| Backdoor.Snowdoor | N/A | CyberNotes-2003-04 |
| Backdoor.Socksbot | N/A | CyberNotes-2003-06 |
| Backdoor.SubSari.15 | 15 | CyberNotes-2003-05 |
| Backdoor.SubSeven.2.15 | 2.15 | CyberNotes-2003-05 |
| **Backdoor.Syskbot** | **N/A** | **Current Issue** |
| Backdoor.SysXXX | N/A | CyberNotes-2003-06 |
| Backdoor.Talex | N/A | CyberNotes-2003-02 |
| Backdoor.Tankedoor | N/A | CyberNotes-2003-07 |
| **Backdoor.Trynoma** | **N/A** | **Current Issue** |
| Backdoor.Turkojan | N/A | CyberNotes-2003-07 |
| Backdoor.Udps.10 | 10 | CyberNotes-2003-03 |
| Backdoor.Unifida | N/A | CyberNotes-2003-05 |
| Backdoor.Upfudoor | N/A | CyberNotes-2003-01 |
| Backdoor.VagrNocker | N/A | CyberNotes-2003-01 |
| Backdoor.Vmz | N/A | CyberNotes-2003-01 |
| Backdoor.Xenozbot | N/A | CyberNotes-2003-01 |
| Backdoor.Xeory | N/A | CyberNotes-2003-03 |
| **Backdoor.XTS** | **N/A** | **Current Issue** |
| Backdoor.Zdemon | N/A | CyberNotes-2003-02 |
| Backdoor.Zdown | N/A | CyberNotes-2003-05 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Zix | N/A | CyberNotes-2003-02 |
| **Backdoor.Zombam** | **N/A** | **Current Issue** |
| Backdoor.Zvrop | N/A | CyberNotes-2003-03 |
| Backdoor-AFC | N/A | CyberNotes-2003-05 |
| Backdoor-AOK | N/A | CyberNotes-2003-01 |
| BackDoor-AQL | N/A | CyberNotes-2003-05 |
| BackDoor-AQT | N/A | CyberNotes-2003-05 |
| BackDoor-ARR | ARR | CyberNotes-2003-06 |
| Backdoor-ARU | ARU | CyberNotes-2003-06 |
| BackDoor-ARX | ARX | CyberNotes-2003-06 |
| BackDoor-ARY | ARY | CyberNotes-2003-06 |
| BackDoor-ASD | ASD | CyberNotes-2003-07 |
| BackDoor-ASL | ASL | CyberNotes-2003-07 |
| **BackDoor-ASW** | **ASW** | **Current Issue** |
| BDS/AntiPC | N/A | CyberNotes-2003-02 |
| BDS/Backstab | N/A | CyberNotes-2003-02 |
| BDS/Ciadoor.10 | 10 | CyberNotes-2003-07 |
| BDS/Evolut | N/A | CyberNotes-2003-03 |
| Daysun | N/A | CyberNotes-2003-06 |
| **DDoS-Stinkbot** | **N/A** | **Current Issue** |
| DoS-iFrameNet | N/A | CyberNotes-2003-04 |
| Downloader-BO.dr.b | N/A | CyberNotes-2003-02 |
| Downloader-BS | N/A | CyberNotes-2003-02 |
| Downloader-BW | N/A | CyberNotes-2003-05 |
| Downloader-BW.b | BW.b | CyberNotes-2003-06 |
| Downloader-BW.c | BW.c | CyberNotes-2003-07 |
| Exploit-IISInjector | N/A | CyberNotes-2003-03 |
| **Gpix** | **N/A** | **Current Issue** |
| Hacktool.PWS.QQPass | N/A | CyberNotes-2003-06 |
| ICQPager-J | N/A | CyberNotes-2003-05 |
| IRC/Backdoor.e | E | CyberNotes-2003-01 |
| IRC/Backdoor.f | f | CyberNotes-2003-02 |
| IRC/Backdoor.g | g | CyberNotes-2003-03 |
| IRC/Flood.ap | N/A | CyberNotes-2003-05 |
| IRC/Flood.bi | N/A | CyberNotes-2003-03 |
| IRC/Flood.br | br | CyberNotes-2003-06 |
| **IRC/Flood.bu** | **bu** | **Current Issue** |
| IRC-Emoz | N/A | CyberNotes-2003-03 |
| IRC-OhShootBot | N/A | CyberNotes-2003-01 |
| JS.Fortnight.B | B | CyberNotes-2003-06 |
| JS.Seeker.J | J | CyberNotes-2003-01 |
| JS/Seeker-C | C | CyberNotes-2003-04 |
| JS_WEBLOG.A | A | CyberNotes-2003-05 |
| KeyLog-Kerlib | N/A | CyberNotes-2003-05 |
| Keylog-Razytimer | N/A | CyberNotes-2003-03 |
| KeyLog-TweakPan | N/A | CyberNotes-2003-02 |
| Linux/Exploit-SendMail | N/A | CyberNotes-2003-05 |
| MultiDropper-FD | N/A | CyberNotes-2003-01 |
| Pac | N/A | CyberNotes-2003-04 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| ProcKill-AE | N/A | CyberNotes-2003-05 |
| ProcKill-AF | N/A | CyberNotes-2003-05 |
| **ProcKill-AH** | **AH** | **Current Issue** |
| ProcKill-Z | N/A | CyberNotes-2003-03 |
| **Proxy-Guzu** | **N/A** | **Current Issue** |
| PWS-Aileen | N/A | CyberNotes-2003-04 |
| PWSteal.AlLight | N/A | CyberNotes-2003-01 |
| **PWSteal.Hukle** | **N/A** | **Current Issue** |
| PWSteal.Rimd | N/A | CyberNotes-2003-01 |
| PWSteal.Senhas | N/A | CyberNotes-2003-03 |
| PWS-Tenbot | N/A | CyberNotes-2003-01 |
| PWS-WMPatch | N/A | CyberNotes-2003-07 |
| QDel359 | N/A | CyberNotes-2003-01 |
| QDel373 | 1373 | CyberNotes-2003-06 |
| Qdel374 | 1374 | CyberNotes-2003-06 |
| Qdel375 | 1375 | CyberNotes-2003-06 |
| Qdel376 | 1376 | CyberNotes-2003-07 |
| **QDel378** | **1378** | **Current Issue** |
| Renamer.c | N/A | CyberNotes-2003-03 |
| **Reom.Trojan** | **N/A** | **Current Issue** |
| StartPage-G | G | CyberNotes-2003-06 |
| Stoplete | N/A | CyberNotes-2003-06 |
| Swizzor | N/A | CyberNotes-2003-07 |
| Tellafriend.Trojan | N/A | CyberNotes-2003-04 |
| Tr/Decept.21 | 21 | CyberNotes-2003-07 |
| Tr/DelWinbootdir | N/A | CyberNotes-2003-07 |
| TR/Fake.YaHoMe.1 | N/A | CyberNotes-2003-02 |
| Tr/SpBit.A | A | CyberNotes-2003-04 |
| TR/WinMx | N/A | CyberNotes-2003-02 |
| Troj/Dloader-BO | N/A | CyberNotes-2003-02 |
| Troj/Manifest-A | N/A | CyberNotes-2003-03 |
| Troj/Qzap-248 | N/A | CyberNotes-2003-01 |
| Troj/SadHound-A | N/A | CyberNotes-2003-03 |
| Troj/Slacker-A | A | CyberNotes-2003-05 |
| Troj/Slanret-A | N/A | CyberNotes-2003-03 |
| Troj/TKBot-A | A | CyberNotes-2003-04 |
| TROJ_JBELLZ.A | A | CyberNotes-2003-02 |
| TROJ_KILLBOOT.B | B | CyberNotes-2003-01 |
| TROJ_RACKUM.A | A | CyberNotes-2003-05 |
| **Trojan.AprilFool** | **N/A** | **Current Issue** |
| Trojan.Barjac | N/A | CyberNotes-2003-05 |
| Trojan.Dasmin | N/A | CyberNotes-2003-01 |
| Trojan.Dasmin.B | B | CyberNotes-2003-03 |
| Trojan.Downloader.Aphe | N/A | CyberNotes-2003-06 |
| Trojan.Downloader.Inor | N/A | CyberNotes-2003-02 |
| Trojan.Grepage | N/A | CyberNotes-2003-05 |
| **Trojan.Guapeton** | **N/A** | **Current Issue** |
| Trojan.Idly | N/A | CyberNotes-2003-04 |
| Trojan.Ivanet | N/A | CyberNotes-2003-02 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Trojan.KKiller | N/A | CyberNotes-2003-01 |
| Trojan.Poldo.B | B | CyberNotes-2003-02 |
| Trojan.Poot | N/A | CyberNotes-2003-05 |
| Trojan.ProteBoy | N/A | CyberNotes-2003-04 |
| Trojan.PSW.Gip | N/A | CyberNotes-2003-06 |
| Trojan.PSW.Platan.5.A | N/A | CyberNotes-2003-01 |
| Trojan.PWS.QQPass.D | N/A | CyberNotes-2003-02 |
| Trojan.Qforager | N/A | CyberNotes-2003-02 |
| Trojan.Qforager.Dr | N/A | CyberNotes-2003-02 |
| Trojan.Qwe | N/A | CyberNotes-2003-02 |
| Trojan.Snag | N/A | CyberNotes-2003-02 |
| Trojan.Unblockee | N/A | CyberNotes-2003-01 |
| Uploader-D | D | CyberNotes-2003-06 |
| Uploader-D.b | D.b | CyberNotes-2003-07 |
| VBS.Kasnar | N/A | CyberNotes-2003-06 |
| VBS.Moon.B | B | CyberNotes-2003-02 |
| VBS.StartPage | N/A | CyberNotes-2003-02 |
| VBS.Trojan.Lovcx | N/A | CyberNotes-2003-05 |
| VBS/Fourcourse | N/A | CyberNotes-2003-06 |
| W32.Benpao.Trojan | N/A | CyberNotes-2003-04 |
| W32.CVIH.Trojan | N/A | CyberNotes-2003-06 |
| W32.Socay.Worm | N/A | CyberNotes-2003-02 |
| W32.Systentry.Trojan | N/A | CyberNotes-2003-03 |
| W32.Xilon.Trojan | N/A | CyberNotes-2003-01 |
| W32.Yinker.Trojan | N/A | CyberNotes-2003-04 |
| W32/Igloo-15 | N/A | CyberNotes-2003-04 |
| Xin | N/A | CyberNotes-2003-03 |

**AprilNice:** The purpose of this Trojan is to simply rename you Outlook Inbox to "April Fools Again" and change various Windows system policies. When executed this Trojan will do the following:

- Minimizes all active windows
- Automatically launches the Outlook client
- Renames your Outlook inbox to "April Fool Again"

The registry settings for the following keys are been set to (1):

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer "NoClose" (Opens a window that cannot be closed)
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer "NoLogoff" (Disables the client from logging off)
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system "DisableChangePassword" (Disables the client from changing passwords)
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system "DisableLockWorkstation" (Disables the user from locking the workstation)
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system "DisableTaskMgr" (Disables the task manager)

**BackDoor-ASW:** This is a backdoor Trojan that operates in stealth mode. It hides its processes, directory, files, and registry keys. When run, it installs itself as a service on the victim's machine. The following keys are created and visible:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RTKIT
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_NPF

Other registry keys associated with these services are hidden. It creates various directories and files. These files are also hidden. They are visible if the system is in safe mode. In safe mode, a service named "RtKit" is also visible. The backdoor can communicate with the client in 4 ways (userdefined, ICMP, UDP, TCP). In TCP mode, it can use any open port on the machine. Default port is 445. The backdoor can perform various malicious operations on the victim's machine.

**Backdoor.EggDrop (Aliases: Backdoor.EggDrop.130, Backdoor.EggDrop.14, Backdoor.EggDrop.149):** This is a Backdoor Trojan that gives a malicious user access to your computer. It contains three modules:

- Server editor
- Injector
- Backdoor

It attempts to inject the backdoor module into a configurable process. When Backdoor.EggDrop runs, it starts a configurable service and injects the backdoor module into a configurable process. The Trojan informs the malicious user by e-mail or ICQ and listens on a configurable port and waits for commands from the malicious user.

**Backdoor.FTP_Ana.D:** This is a Backdoor Trojan that gives a malicious user unauthorized access to your computer. This Trojan copies itself as the file Net.exe. When Backdoor.FTP_Ana.D runs, it copies itself as %Windir%\net.exe and creates the value, "net"="%Windir%\net.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. Next is creates the value, "StubPath"="%Windir%\net.exe ASC,' in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\Net

It notifies the client side using the ICQ pager and waits for commands from the remote client. The commands give a malicious user full access to the file system of the infected computer.

**Backdoor.Graybird.B (Alias: Backdoor.Delf.eb):** This is a variant of Backdoor.Graybird. It gives a malicious user unauthorized access to your computer. The existence of the file Svch0st.exe is an indication of a possible infection. This threat is written in Delphi and compressed with ASPack. When Backdoor.Graybird.B runs, it copies itself as %System%\Svch0st.exe and creates the value, "svchost"="%System%\Svch0st.exe," in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also changes the (Default) value to, "%system%\SVCH0ST.EXE "%1" %*," in the registry key:

- HKEY_CLASS_ROOT\exefile\shell\open\command

so that the Trojan runs when you execute the .exe files. If the operating system is Windows NT/2000/XP, the Trojan also creates the value, "run"="%system%\svch0st.EXE," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

If the operating system is Windows 95/98/ME, the Trojan adds the line:

- run=C:\WINDOWS\SYSTEM\SVCH0ST.EXE

to the [windows] section of the Win.ini file, so that the Trojan runs when you start Windows. Then, it attempts to access the password cache stored on your computer. The cached passwords include the modem and dialup passwords, URL passwords, share passwords, as well as others. The Trojan intercepts keystrokes, which could allow Backdoor.Graybird.B to steal confidential information. Once Backdoor.Graybird is installed, it waits for the commands from the remote client. These commands allow the malicious user to perform various actions.

**Backdoor.Graybird.C:** This is a Backdoor Trojan and a variant of Backdoor.Graybird. It gives a malicious user unauthorized access to your computer. It opens port 52013 to listen for commands. The existence of the file, HGZSERVER.EXE, is an indication of a possible infection. The Trojan uses a text file icon to attempt to disguise itself as an ordinary .txt file. This threat is written in Delphi. When

Backdoor.Graybird.C runs, it copies itself as %System%\HgzServer.exe and creates the value, "huigezi %System%\HgzServer.exe," in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. If the operating system is Windows 95/98/ME, the Trojan adds the line, "run=%System%\HgzServer.exe," to the [windows] section of the Win.ini file so that the Trojan runs when you start Windows. It starts an FTP server on port 21, which allows the malicious user to use the compromised computer as a temporary storage device and listens on port 52013 and waits for the commands from the malicious user to perform unauthorized actions.

**Backdoor.Monator (Alias: Backdoor.Monator.20):** This is a Backdoor Trojan that gives a malicious user full access to your computer. By default it opens port 8811 for listening. The Backdoor is written in Microsoft Visual Basic, version 6. When Backdoor.Monator is executed, it opens port 8811 and gives malicious users full access to your computer. The backdoor can also steal AOL Instant Messenger information, such as your screen name and password. This Trojan does not drop any files or modify registry keys.

**Backdoor.Sdbot.G**: This is a Backdoor Trojan that is a variant of Backdoor.Sdbot. It allows a malicious user to use Internet Relay Chat (IRC) to gain access to your computer. The existence of the file Svost.exe is an indication of a possible infection. It is compressed with UPX. The unpacked size is about 232 KB. When Backdoor.Sdbot.G runs, it copies itself as: %System%\Svost.exe and adds the value, "Svost Loader"="svost.exe," to the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunServices

It uses its own IRC client to connect to a specified IRC channel and waits for the commands to perform various malicious actions.

**Backdoor.Syskbot:** This is a Backdoor Trojan Horse that gives a malicious user access to your computer. When Backdoor.Syskbot is executed, it copies itself to C:\Windows\Sysk4.exe and adds the string value, "Webadmin"="C:\Windows\Sysk4.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

The Trojan opens TCP ports 1482 to 1485. It can do the following:

- Control your IRC client if one is installed.
- Send the Trojan to other IRC channels and attempt to compromise more computers.
- Perform Denial of Service (DoS) attacks against a target defined by the malicious user.
- Steal password files

**Backdoor.Trynoma (Alias: Backdoor.VB.fm):** This is a typical Backdoor Trojan that gives a malicious user full access to your computer. The presence of the file, Windll.exe, on your computer may be an indication of infection. When Backdoor.Trynoma is executed, it copies itself as %System%\Windll.exe and creates the string values:

- "Windll"="%system%\Windll.exe"
- "KavRuns"="%system%\Windll.exe"

in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Backdoor.Trynoma allows a malicious user to:

- Copy files to and from your computer.
- Execute programs.
- Take a screen shot of your Windows desktop.

**Backdoor.XTS (Alias: Backdoor-ASL):** This is a Backdoor Trojan that gives a malicious user access to your computer. The Trojan runs only on Windows NT/2000/XP and adds a service to the compromised system. The main module, Svchost.exe, is packed with UPX. When Backdoor.XTS is executed, it drops the following files:

- %Windows%\Svchost.exe
- %System%\Extapi.dll
- %System%\Sysmsg.dll
- %System%\Rascfg.dll

and adds the new services:

- Name: System Important Message.
- Path: %Windows%\Svchost.exe -k ras.

It injects Extapi.dll and Sysmsg.dll into the program described in Rascfg.dll. By default, the Trojan injects them into the file, Explorer.exe and drops the log file, %System%\Word.dll. Backdoor.XTS has the capability to:

- Give the malicious user access to your computer.
- Steal information.
- Send e-mails.
- Capture keystrokes.
- Hook specific APIs.

**Backdoor.Zombam (Alias: Backdoor.Zombam.d):** This is a Backdoor Trojan that gives a malicious user access to your computer, via a Web browser. The Trojan attempts to terminate various antivirus and firewall processes. The existence of the file Ckmgr.exe is an indication of a possible infection. This Trojan opens port 80, by default. When Backdoor.Zombam is executed, it copies itself as the following files, depending on the operating system:

- Windows 95/98/Me: %Windir%\Cookies\Ckmgr.exe
- Windows NT/2000/XP: Document and Settings\<user name>\Cookies\Ckmgr.exe.

and adds the value, “ckmgr"="%Windows%\Cookies\ckmgr.exe,” or “ckmgr"="Document and Settings\<user name>\Cookies\ckmgr.exe,” to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The Trojan opens port 80, by default, to give unauthorized access to a malicious user, by using a Web browser and attempts to terminate various antivirus and firewall processes.

**DDoS-Stinkbot:** This Trojan is an IRC bot that is controlled by a remote malicious user to use infected systems to initiate a Distributed Denial of Service attack against others. When run, it copies its components to the SYSTEM directory with the following filenames:

- SETUPINF.EXE (Server component)
- WINVIDEO.EXE (Flooding component)

The dropper file received by AVERT also included the following additional application, and two common Microsoft files:

- PSKILL.EXE (detected as PSKill application)
- MSVBVM60.DLL (1,388,544 bytes)
- MSWINSCK.OCX (108,336 bytes)

It does not create a registry key or any entries in INI files to load itself at startup. Once infected, the local system "reports in" to a specified IRC server so that a malicious user can issue commands. A malicious user can also instruct the bot to download and run other programs, remotely. This Trojan’s components pose as valid Windows system files.

**Gpix:** This is an adware Trojan that displays adult content advertising based on the websites visited by the infected user. When run, it displays a fake error message. The Trojan then copies itself to the WINDOWS SYSTEM (%SysDir%) as shellexpl.exe, creates a registry run key to load itself at system startup, and exists.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
  Run "Explorer" = C:\WINDOWS\SYSTEM\shellexpl.exe en

The Trojan deletes all cookies in the cookies folder and then monitors newly created cookies that contain numerous words. When a cookie is created that contains these words, an adult website is contacted, and

advertisements are displayed on the infected system. The Trojan makes use of 2 configuration files, also in the %SysDir% folder.

- hndldt.ini
- winhndl.ini

**IRC/Flood.bu:** This description is intended as a general guide. The malicious user who creates the dropper file or uses the Trojan decides the specific actions taken. This is an Internet Relay Chat BOT/DDoS tool. It is dropped by a self-extracting archive that includes a copy of the mIRC client within itself. This allows users who do not run mIRC to become used in a DDoS attack. When run, the dropper creates a directory and extracts several files to it. The extracted files are in the following categories:

- IRC script instruction for various Trojan activities.
- mIRC configuration file.
- Batch file to perform remote login, remote launches.
- mIRC executable for remote connection and remote access.
- HideWindow application to hide the mIRC window.
- RemoteProcessLaunch application to launch EXEs.

The batch file (username, password) uses various username/password combinations. The dropper file received by AVERT created a registry entry to run again at Windows startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "NTFix" = %Trojan File%
  (the path for the file being the directory where the dropper file was initially run from)

Infected machines should be carefully examined, since IRC/Flood droppers are often repackaged with new files, so it is possible that a malicious user has installed further hacktools or backdoors. If mIRC is already installed on a system, registry entries pointing to the installed product will be redirected to the version dropped by the Trojan.

**ProcKill-AH:** This Trojan attempts to terminate the process of programs that could be used to find or remove malware. It searches running processes with various strings to terminate those programs relating to security and gathering system information. This Trojan adds itself to the Windows directory as MEMCHECK.exe, and it creates the following registry key to run itself at Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Memory Check" = %WinDir%\MEMCHECK.exe

Infected machines should be carefully examined, since ProcKill Trojans are often dropped with other Trojans, so that it can mask their malicious activities.

**Proxy-Guzu:** This Trojan allows a remote user to send e-mail through the infected system. Such actions may be used by SPAMMERS to send a large number of messages anonymously. When run, the Trojan opens a TCP port for listening. It then sends an e-mail using its own SMTP engine, and Hotmail servers. The message sent is as follows:

- From: fakeaddress@hotmail.com
- To: phishinc@hotmail.com
- Subject: Infected user's IP address:TCP port opened by Trojan

A registry run key is also created to load the Trojan at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "Services" = Execution path of Trojan

**PWSteal.Hukle (Alias: Trojan.PSW.Hukle.a):** This is a Trojan Horse that tries to log keystrokes and send the information to the malicious user. The existence of the file Hiddukel.exe is an indication of a possible infection. When PWSteal.Hukle is run, it creates the files:

- %System%\Hiddukel.exe
- %System%\Hiddukel.dll

It modifies the value, “(Default)""%1" %*,” to, “(Default)"C:\WINDOWS\SYSTEM\hiddukel.exe" "%1" %*" in the registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command

so that the Trojan runs each time you run a .exe file. The stolen information is sent to a malicious user.

**QDel378:** This Trojan hides all commands from appearing on the on the screen and blocks the user from sending a command to halt the batch from executing. It overwrites the "autoexec.bat" with a file named "fotos.bat" and deletes all folders from the root of the C drive.

**Reom.Trojan:** This is a simple program that sends an inappropriate message written in Chinese to all the computers in the work group. When Reom.Trojan is run, it displays a dialog box with a YES and NO button, but it will fix the mouse cursor over the YES button, preventing a user from clicking anything else. When you click YES, Reom.Trojan will execute the command: "net send * <message>" whereby <message> is a vulgar text in Chinese. This command sends the <message> to all the computers in the same work group as your computer. Also, it is only available under Windows NT/2000/XP and will therefore fail on Windows 95/98/ME.

**Trojan.AprilFool:** This is a Trojan Horse that is written in Microsoft Visual Basic 6. In order for it to execute, the Visual Basic (VB) run-time libraries must be installed on your computer. Trojan.AprilFool works only if Microsoft Exchange is installed. The Trojan may rename your Microsoft Outlook or Outlook Express Inbox to "April Fool."

**Trojan.Guapeton (Alias: Trojan.Win32.Guapeton, Guapeton):** This is a malicious program that deletes all the file icons on your computer. When Trojan.Guapeton runs, it prompts you to allow the program to run at Startup. If you click OK, the Trojan adds the registry value, "EatIcons"="<path/file name of Trojan> /SILENT," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

and asks you whether you want to delete the icons now. If you click Yes, the Trojan deletes all the file icons on the computer.